IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: David E. MCDYSAN	
Application No.: 10/023,043	Group Art Unit: 2135
Filed: December 17, 2001	Examiner: Gyorfi, T.
Attorney Docket: RIC01059 Client Docket: 09710_1203	

For: SYSTEM, METHOD AND APPARATUS THAT EMPLOY VIRTUAL PRIVATE NETWORKS TO RESIST IP QoS DENIAL OF SERVICE ATTACKS

REPLY BRIEF

Honorable Commissioner for Patents
Alexandria, VA 22313-1450

Dear Sir:

This Reply Brief is submitted in response to the Examiner's Answer mailed June 22, 2007.

I. STATUS OF THE CLAIMS

Claims 1-24 are pending and are on appeal.

II. GROUNDS OF REJECTION TO BE REVIEWED

Whether claims 1, 3-9, 11-16, and 18-22 are anticipated under 35 U.S.C § 102 (b) based on *Seid et al.* (US 5,768,271)?

Whether claim 23 is obvious under 35 U.S.C § 103 based on *Seid et al.* (US 5,768,271)?

Whether claims 1-24 are obvious under 35 U.S.C § 103 based on Admitted Prior Art (*APA*) in view of *Seid et al.* (US 5,768,271)?

III. ARGUMENT

Appellant maintains and incorporates the positions presented in the Appeal Brief filed February 16, 2007, but presents further refutation of certain assertions presented in the Examiner's Answer.

At pages 13-14 *et seq.* of the Answer, the Examiner quotes language by Appellant arguing that the claimed network system comprises first and second access network logical connections and that the first logical connection (for intra-VPN traffic) and the second logical connection (for extra-VPN traffic) are both within the VPN. The Examiner contends that Appellant's argument is predicated upon a logical contradiction because "the VPN contains traffic that by its very definition cannot be part of the VPN!" (Answer-page 14). The Examiner further calls Appellant's argument "a red herring" and contends that there is no basis in the specification or the claims for concluding that **both** logical connections, especially the second logical connection comprising the extra-VPN traffic, are part of the VPN. Appellant respectfully, but vehemently, disagrees.

Specific reference to Figure 3 and pages 9-10 of the specification, describing Figure 3, refutes the Examiner's argument. The instant invention, as claimed, prevents a Denial of Service (DoS) attack from sites outside the Virtual Private Network (VPN) by directing intra-VPN traffic to a first logical port 27 on access link 1, of boundary router 22a, while directing traffic from other VPNs or other sites to a second logical port 28 on access link 1 of boundary router 22a. Thus, there is a first logical connection for intra-VPN traffic and a second logical connection for

all extra-VPN traffic. Contrary to what the Examiner's argument suggests, i.e., that the claims require the extra-VPN traffic to be a part of the VPN, the claims do not require traffic to be a part of the VPN. Rather, the claims recite that the VPN comprises one or more egress routers having connections to an access network. These egress routers function in a different manner, depending on whether the traffic they transmit is intra-VPN traffic or extra-VPN traffic. The egress routers transmit intra-VPN traffic to a destination host belonging to the VPN from sources within the VPN within a first logical connection for intra-VPN traffic. However, the egress routers transmit all extra-VPN traffic to the destination host from sources outside the VPN within a second logical connection for extra-VPN traffic. The first and second logical connections are separate from each other. This is clearly recited in independent claim 1, for example.

As explained at page 10 of the specification, each boundary router 22 prioritizes intra-VPN traffic over extra-VPN traffic, or allocates access link capacity such that extra-VPN traffic cannot interfere with inter-VPN traffic. This precedence-granting scheme is achieved by a special configuration of network elements and protocols, including partitioning of the physical access between intra-VPN and extra-VPN traffic. By contrast, the prior art, exemplified by the *Seid et al.* reference, does not segregate traffic destined for sites within the same VPN (i.e., intra-VPN traffic) from traffic sent from other regions (i.e., extra-VPN traffic).

It is the Examiner's argument that is the "red herring" because the claims do not require, and Appellant does not argue, that the intra-VPN traffic and extra-VPN traffic, per se, are part of the VPN. Rather, Appellant argues, and has argued, that the traffic in a particular VPN is separated or partitioned based on the source of the traffic, i.e., whether the traffic originated within the VPN (intra-VPN) or outside of the VPN (extra-VPN). It is this **strategic partitioning** of intra-VPN and extra-VPN traffic and the transmission of intra-VPN traffic and extra-VPN

traffic to **different** access network logical connections within the VPN to prevent DoS attacks on the access link originating from sources outside the VPN which is a claimed concept that is neither disclosed nor suggested by *Seid et al.*

Contrary to the Examiner's allegation at page 15 of the Answer, Appellant did not and does not argue that traffic is partitioned **within a VPN** into intra-VPN and extra-VPN traffic. Rather, the traffic is already either intra-VPN or extra-VPN when received by the ingress routers. What the present invention does is logically partition the intra-VPN and extra-VPN traffic utilizing a network-based VPN protocol, such that the traffic is transmitted to different access network logical connections within the VPN based on whether the traffic is intra-VPN traffic or extra-VPN traffic.

At page 17 of the Answer, the Examiner uses column 15, lines 10-25, of *Seid et al.* as a basis for contending that the reference teaches distinguishing between intra-VPN and extra-VPN traffic and treating them differently. While this portion of the reference discusses the determination of specific end point locations of Virtual Paths (VPs), and providing an identity of a VPN to which the VP will belong, etc., it discusses nothing that would have been suggestive of segregating, within the same VPN, intra-VPN traffic from extra-VPN traffic. While *Seid et al.* identifies, at column 4, lines 1-10, that packets to different VPNs are specifically identified, such identification is not performed on the basis of whether they originated within a particular VPN or without a particular VPN, as in the claimed invention.

Notwithstanding the Examiner's request, at page 18 of the Answer, for Appellant to provide evidence that *Seid et al.* discloses transmitting traffic from one VPN to another VPN, it is the Examiner who has the burden of proof of establishing anticipation under 35 U.S.C. § 102 and obviousness under 35 U.S.C. § 103. Appellant is under no obligation to provide evidence one

way or another until and unless the Examiner has established a *prima facie* case. For the reasons elucidated in the Appeal Brief and for the reasons discussed above, no *prima facie* case has been established either under 35 U.S.C. § 102 or 35 U.S.C. § 103 because *Seid et al.* **nowhere** discloses or suggests **the notion of partitioning or segregating traffic from sites within the same VPN (intra-VPN traffic) from traffic without that VPN (extra-VPN traffic), and applying a protocol that prioritizes intra-VPN traffic over extra-VPN traffic, or allocates access link capacity such that extra-VPN traffic cannot interfere with intra-VPN traffic.**

The various passages of *Seid et al.* recited by the Examiner at pages 20-22 of the Answer, viz., column 10, lines 20-30, and 38-50, and column 12, lines 20-30, do not suggest the partitioning or segregating of traffic as claimed by Appellant. Those cited passages are directed to congestion control by a VPN and while the congestion control of *Seid et al.* is carried out on a per VPN basis so that congestion outside of a VPN's logical domain does not affect the performance of the VPN (see, e.g., the abstract of *Seid et al.*), there is absolutely no disclosure or suggestion in *Seid et al.* that the congestion control is implemented in any manner so as to result in partitioning or segregating traffic from sites within the same VPN (intra-VPN traffic) from traffic without that VPN (extra-VPN traffic), and applying a protocol that prioritizes intra-VPN traffic over extra-VPN traffic, or allocates access link capacity such that extra-VPN traffic cannot interfere with intra-VPN traffic, as required by the claims on appeal.

Accordingly, since the Examiner relies on *Seid et al.* for a teaching that is non-existent in *Seid et al.*, all of the Examiner's rejections under 35 U.S.C. § 102 and 35 U.S.C. § 103 must fall.

IV. CONCLUSION AND PRAYER FOR RELIEF

The claims require partitioning or segregating traffic from sites within the same VPN (intra-VPN traffic) from traffic without that VPN (extra-VPN traffic), and applying a protocol that prioritizes intra-VPN traffic over extra-VPN traffic, or allocates access link capacity such that extra-VPN traffic cannot interfere with intra-VPN traffic, but *Seid et al.* neither discloses nor suggests such a feature. Appellant, therefore, requests the Honorable Board to reverse each of the Examiner's rejections.

Respectfully Submitted,

DITTHAVONG MORI & STEINER, P.C.

8/14/07
Date

Phouphanomketh Dittahvong
Attorney for Applicant(s)
Reg. No. 44658

918 Prince Street
Alexandria, VA 22314
Tel. 703-519-9952
Fax.703-519-9958